REMARKS

Claims 1-19 remain pending in the instant application (hereinafter, the '852 Application). Claim 2 has been amended to recite '...authenticating...' Support for this amendment may be found, for example, in paragraph [0020]. Claims 15 and 18 have been amended to recite 'performing an initial assessment of the electronic network.' Support for these amendments may be found, for example, at in claim 1 and paragraph [0020]. No new matter has been added to the claims by these amendments.

Applicants submit that the following remarks attend to all issues presented in the Office Action dated June 04, 2007. Where used herein, numbered subtitles reflect the numbering of issues presented in the aforementioned the Office Action.

3-4. Claim Rejections – 35 U.S.C. § 102

Claims 15-19 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0015719 (hereinafter, "Lee"). Applicants respectfully traverse.

In order to anticipate claims 15-19, Lee must teach every element of each claim and "the ***identical invention*** must be shown in as complete detail as contained in the ... claim." *MPEP 2131*, citing *Verdegaal Bros. V. Union Oil Co. of California*, 814 F.2d 628, 2 USPQ2d 1051 (Fed. Cir. 1987) and *Richardson v. Suzuki Motor Co.*, 868 F2.d 1226, 9 USPQ2d 1913 (Fed. Cir. 1989), emphasis added. However, Lee does not teach or suggest each and every claim limitation within claims 15-19, as required by 35 U.S.C. § 102(e).

Regarding Independent Claim 15: Amended claim 15 states a system for event monitoring, comprising:

(1) an electronic network, having cooperative agent network for performing an initial assessment of the electronic network, for collecting events;

(2) one or more event correlation engines, each event correlation engine

(a) being connected to the electronic network and

(b) having a receive event handler for receiving events addressed to the event correlation engine; and

(3) one or more event correlation modules,

(a) each of the event correlation modules having an event pattern that defines events of interest,

(b) each of the correlation modules receiving all events received by the event correlation engine,

(c) the event correlation module correlating the events of interest.

Lee does not disclose an electronic network having cooperative agent network for performing an initial assessment of the electronic network. The Examiner also acknowledges on page 5 of the Office Action that Lee does not explicitly teach this feature, thus anticipation for claim 15 is not established. Reconsideration for claim 15 is respectfully requested.

Regarding Dependent Claims 16-17: Claims 16-17 depend on claim 15 and benefit from the same argument. Reconsideration for claims 16-17 is respectfully requested.

Regarding Independent Claim 18: Amended claim 18 states a method of pattern recognition, comprising:

(1) performing an initial assessment of the electronic network,

(2) collecting electronic network events; sampling the electronic network events with one or more event correlation engines;

(3) passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine;

(4) comparing events in each of the event correlator modules by sampling the events,

(5) determining if any of the events matches an event pattern, and, if there is a match,

(6) creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution; and

(7) determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution.

Lee does not disclose the step of performing an initial assessment of the electronic network as required by step 1 of claim 18. The Examiner also acknowledges on page 5 of the

Office Action that Lee does not explicitly teach this feature, thus anticipation of claim 18 has not been established. Reconsideration for claim 18 is respectfully requested.

Regarding Dependent Claim 19: Claim 19 depends on claim 18 and benefits from the same argument. Reconsideration for claim 19 is respectfully requested.

5-6. Claim Rejections – 35 U.S.C. 103 – Lee in view of Ghosh

Claims 1-9 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lee in view of U.S. Patent No. 7,181,768 (hereinafter, "Ghosh"). Applicants respectfully traverse.

Lee discloses an intelligent security engine (ISE) is for analyzing an alert message, a traffic information and event information transferred from the plurality of security agents to decide if there is an attack and to generate a signature through a learning process. A security policy manager (SPM) manages and applies a security policy to each of the plurality of security agents based on the decision of the ISE. The ISE performs a correlation analysis and a causation analysis on suspicious traffic and events and a detection message transferred from the plurality of security agents. Further, the ISE carries out a pattern analysis and generates a new detection pattern through a self-learning process (see Lee Specification, paragraphs [0013] – [0014]). Lee does not disclose performing an initial assessment of the electronic network to determine normal activity.

Ghosh discloses an intrusion detection system (IDS) that uses application monitors for detecting application-based attack against the computer systems. The IDS, for each application in the session, compares a data string, in the order in which it was generated, with an associated model application profile. For a segment, the data string counter tracks the number of data strings that are not found in the model profile for the application. If the ratio of such data strings to the total number of data strings in a segment exceeds a pre-determined data string threshold, the segment is labeled anomalous. Similarly, for each anomalous segment in an application profile for a session, a segment counter is incremented. If the ratio of the number of anomalous segments to the total number of segments in the application profile exceeds a segment threshold, the application is labeled anomalous. Ghosh does not have one or more agents within components of the electronic network nor does Ghosh **perform an initial assessment** of the electronic network to determine normal activity.

Regarding Independent Claim 1: Claim 1 states a method of protecting an electronic network, comprising:

(a) installing one or more agents within components of the electronic network

(b) monitoring the electronic network for abnormal activity using the agents; and

(c) protecting the electronic network by blocking the abnormal activity using the agents

(d) **performing an initial assessment** of the electronic network to determine normal activity.

Prima facie obviousness has not been established against claim 1. For example, as the Examiner has already pointed out, and applicants agree, that Lee does not disclose step (d) of claim 1. Adding Ghosh does not remedy the failings of Lee, because Ghosh also fails to disclose performing an initial assessment of the electronic network to determine normal activity.

Additionally, there can be no motivation to combine Ghosh with Lee because Ghosh teaches away from Lee. For example, Lee discloses "anomaly detection is required to be capable of differentiation normal user behavior, anomalous acceptable behavior, and intrusive behavior." See Lee Specification, paragraph [0045]. In contrast, Ghosh teaches away from Lee by stating "a disadvantage of anomaly detection systems is their inability to identify the exact nature of attack...anomaly detection systems have been prone to excessive false positive identifications because any departure from normal operations is flagged as a positive attack." See Ghosh col. 3 lines 7-15. Because Ghosh is here expressly teaching away from the very motivation the Examiner asserts to be present to combine the reference with Lee, there is no motivation for one of ordinary skill in the art to combined Ghosh with Lee.

It is further noted that the Examiner has misread the Ghosh reference, as demonstrated, for example, on page 5 of the Office Action. The Examiner cites col. 2, lines 10-14 of Ghosh stating "defining normal behavior in anomaly detection by first building user profiles based on the sequence of each user's normal command execution." However, in col. 2 lines 24-30, Ghosh points out "a ***drawback*** to such ***user-based IDS*** is that a user may slowly change his or her behavior to skew the profiling system such that intrusive behavior is deemed normal for that user. Moreover, user-based IDS raises ***privacy concerns*** for users in that such a surveillance system monitors users' every move." In other words, Ghosh clearly teaches that the method presented in col. 2 lines 10-14 is **not** a desirable technique. Since Ghosh plainly pointed out the

"***drawback***" of the user profiles method, there can be no motivation for a person with ordinary skill in the art to combine Lee with Ghosh. Significantly, Applicants note that the rejection fails to assert where Ghosh ever teaches the combination proposed by the Examiner.

Moreover, it is more advantageous for monitoring the electronic network by performing an initial assessment of the electronic network to determine the normal activity because as Ghosh points out the user-based IDS may be skewed if the user changes his or her behavior and privacy concern for the user. Such novel, useful, and undisputed advantages are themselves sufficient to overcome even a proper obviousness rejection.

In summary, Lee and Ghosh, alone or in combination fail to teach or suggest all of the elements of claim 1, and, for at least this reason, cannot substantiate a case of prima facie obviousness. ("To establish a *prima facie* obviousness of a claim invention, all the claim limitations must be taught or suggested by the prior art." *In re Royka*, 490 F. 2d 981, 180 USPQ 580 (CCPA 1974).) There is also no motivation to combine Lee with Ghosh in the manner suggested by the Examiner, nor an expectation of successfully rendering the method of protecting an electronic network of claim 1. Withdrawal of the 130 rejection, and allowance of claim 1 are respectfully requested.

Regarding Dependent Claims 2-9: Claims 2-9 depend from claim 1 and benefit from the same argument. Furthermore, these claims contain additional features that patentably distinguish over Lee in view of Ghosh. For example, claim 2 states "...the step of installing comprises the step of installing a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents." Lee is silent of having a type 2 super peer agent for authenticating, authorizing and reauthorizing agents. As shown, Lee does not teach or suggest each and every element of claim 2; hence, *prima facie* obviousness is not established.

Claim 3 depends from claim 1 and benefits from the same argument. Moreover, claim 3 states "further comprising logical connecting at least one of the agents into one or more cooperative agent cells." Lee is silent about having logical connecting at least one of the agents into one or more cooperative agent cells. In fact, Lee discloses that "because agents are independent of one another, the implementation is less cumbersome and preferably requires less overall code space." See Lee Specification paragraph [0040]. Since Lee agents are expressly

independent of one another, Lee does not teach the cooperative agent cells as required by claim 3.

As shown, Lee does not teach or suggest each and every element of claims 2-9; hence, *prima facie* obviousness is not established. Withdrawal of the rejection hereto and allowance of claims 2-9, are respectfully requested.

7. Claim Rejections – 35 U.S.C. 103 – Lee in view of Ghosh in view of Moran

Claims 10 and 14 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lee in view of Ghosh, and in view of U.S. Patent No. 7,085,936 B1 (hereinafter, "Moran"). Applicants respectfully traverse.

Moran discloses an intrusion detection system comprises an analysis engine configured to use continuations and apply forward-and backward-chaining using rules. The intrusion detection system also includes a trap system comprising a trap host system in which a virtual cage is established, as described in co-pending U.S. Patent Application 09/615,967 (hereinafter "Lyle"). Lyle discloses a security system having a deception server. A deception server contains false data. A router or firewall is configured to route suspected attackers to the deception server instead of permitting the suspected attacker to access the real computer system or network.

Regarding Independent Claim 14: Claim 14 states a system for protecting an electronic network, comprising:

(1) plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate;

(2) a communications protocol within each cooperative agent cell for

(a) communicating between agents of the cooperative agent cell, and

(b) communicating with cell delegates external to the cooperative agent cell

(3) means for determining normal activity levels of the electronic network;

(4) means for means for detecting malicious activity;

(5) means for isolating compromised components of the electronic network;

(6) means for counter-intelligence to reveal the origin of the malicious activity;

(7) means for repairing damage caused by the malicious activity;

(8) means for determining vulnerabilities in the current protection provided by the plurality of agents; and

(9) means for improving protection to resist future attack on the electronic network.

Lee, Ghosh and Moran fail to disclose, at least, elements (1), (3), and (6) of claim 14. Specifically, Lee, Ghosh and Moran do not disclose the agents being grouped into at least one cooperative agent cell having one cell delegate. Although the Examiner cites paragraph [0056] of Lee as allegedly showing "a net broker 102 undertakes communication gateway, encryption and authentication is installed in each of the agents as a separate execution module. Each agent transfers necessary information to its own net broker of the transmitting agent encrypts and delivers the information to the receiving agent." The present application, on the other hand, specifically discloses "cell delegate filters the event information to remove duplicate and unwanted events, and sends the filtered event information to T2SPA." See, e.g., [0033] – [0034]. Clearly, the net broker of Lee is different than the cell delegate of the present application because the net broker is used only as a communication device but is not able to filter the event information to remove duplicate and unwanted events.

Further, Lee, Ghosh and Moran fail to disclose "means for counter-intelligence to reveal the origin of the malicious activity," as required by element (6) of claim 14. The Examiner acknowledges, on page 10 of the Office Action, that Lee and Ghosh do not explicitly teach this feature. Therefore, applicants respectfully suggest that the Examiner has mistakenly cited paragraph [0051] of Lee against element (6) of claim 14 because the Examiner admits that Lee does not teach this feature on page 10 of the Office Action. Moreover, adding Moran does not remedy the failings of Lee and Ghosh, because Moran discloses having "a router or firewall is configured to route suspected attackers to the deception server instead of permitting the suspected attacker to access the real computer system or network" but is silent about having "means for counter-intelligence to reveal the origin of the malicious activity," as required by element (6) of claim 14.

In summary, Moran, Ghosh and Lee do not teach or suggest each and every element of claim 14. Hence, *prima facie* obviousness has not been established. Withdrawal of the rejection thereto, and allowance of claim 14, are respectfully requested.

Regarding Dependent Claim 10: Claim 10 depends from claim 1 and benefits from the same argument. Furthermore claim 10 states wherein the step of protecting comprises one or more of:

(1) luring a malicious agent that causes abnormal activity into a false appearance of success;

(2) planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent;

(3) isolating electronic network components which have been compromised by the malicious agent; attacking the malicious agent;

(4) formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network;

(5) installing patches to eliminate vulnerabilities in the electronic network;

(6) reassessing the electronic network to detect abnormal operations; and

(7) investigating abnormal operations of the electronic network.

The Examiner acknowledges out that both Lee and Ghosh do not teach elements 1 and 2 of claim 10, and applicants agree. Furthermore, Moran also does not teach "... planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent," as required by element (2) of claim 10.

Moran directs to a co-pending U.S. Patent application No. 09/615,967 (hereinafter, "Lyle") to further explain the trap system. Lyle explains that the trap system is "to ensure that the intruder does not break out of the trap system and gain access to the portions of computer network 202 that are being protected from unauthorized access." See Lyle, Specification col. 7, lines 4-13. In other words, Lyle system has the ability to prevent intruder from entering the computer network, but is silent about having the ability to **"identify the origins of the malicious agent**." Thus, adding Moran and Lyle do not remedy the failures of Lee and Ghosh.

Even when combined, Moran, Lyle, Ghosh and Lee do not teach or suggest each and every element of claim 10. Hence, *prima facie* obviousness has not been established. Withdrawal of the rejection thereto and allowance of claim 10, are respectfully requested.

8. Claim Rejections – 35 U.S.C. 103 – Lee in view of Ghosh in view of Rowland

Claims 11-13 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lee in view of Ghosh, and in view of U.S. Patent No. 7,058,968 (hereinafter, "Rowland"). Applicants respectfully traverse.

Rowland discloses a computer security and management system having generic distributed command, control, and communication framework. The system is designed to allow modularity for easy expansion and flexibility such that most client and server components can be reversed depending upon the role they serve in the system for example, a client may "morph" or change to into server in case of central system failures. The system uses handlers 202-209. Handlers are software code designed to perform one or more specific functions. Handlers are designed to be very focused pieces of code that perform a fixed set of very specific functions. A handler focuses on one area of the system, the number of software errors ("bugs") that are contained in the code may be reduced which optimizes overall system debugging efforts. See Roland Abstract, and Specification col. 6 lines 1-15.

Regarding Dependent claims 11-13: Claims 11-13 depend from claim 3 which depends from claim 1 and benefit from the same argument. Additionally, these claims contain additional features that patentably distinguish over Rowland in view of Lee and Ghosh. For example, claim 11 recites "promoting one of the agents in each of the cooperative agent cells to a cell delegate." In response to the Examiner's assertion that Rowland

> "teaches that the architecture of the system is designed to allow modularity. This modularity allows for the roles to be reversed. In col. 4, lines 44-67. It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of an intelligent security engine and system that utilizes machine learning anomaly detection taught in '012 and '719 to include a means to develop a hierarchical agent installation promoting agents." (Office Action dated June 04, 2007, pages 12-13).

Applicants respectfully disagree. Applicants assume that the Examiner meant to cite Rowland ('968) and not Rowland ('012). It would not be obvious to promote Rowland's "handlers" because Rowland specially discloses that "handlers are designed to be very focused pieces of code that perform a fixed set of very specific functions" such that " the code may be reduced which optimizes overall system debugging efforts." See Rowland Specification col. 6 lines 1-15. The handlers of Rowland are designed to be very focus pieces of code that performs

a fixed set of very specific functions, therefore, the handlers cannot be promoted to perform a different function.

Claim 12 recites "further comprising: promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent; authenticating new agents with the type 1 super peer agent; and communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity." Again, Lee, Ghosh and Rowland fail to disclose these elements of claim 12. As argued above, the Examiner acknowledges that Lee and Ghosh do not have the ability to promote an agent. Adding Rowland does not remedy these failures of Lee and Ghosh because Rowland's handlers are designed to be very focused pieces of code that perform a fixed set of very specific functions. See Rowland col. 6 lines 1-15.

Withdrawal of the rejection thereto and allowance of claims 11-13, are respectfully requested.

CONCLUSION

In view of the above Remarks, Applicants have addressed all issue raised in the Office Action dated June 04, 2007. All pending claims are believed to be allowable. Lee does not anticipate independent claims 15-19, nor do Lee, Ghosh, Moran or Rowland, alone or in combination, establish *prima facie* obviousness over any of the pending claims. Applicants respectfully request a Notice of Allowance for all of claims 1-19.

The Examiner is encouraged to telephone Applicant's attorney, Curtis A. Vock, at (720) 931-3011 to discuss the amendments presented herein, or any outstanding issues regarding the '852 application.

Authorization to charge fees associated with a two-month extension of time is submitted herewith. If any fee is deemed necessary in connection with this Amendment and Response, the Commissioner is authorized to charge the Deposit Account No. 12-0600.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 10/2/07 By: _____

Mimi Nguyen, Reg. No. 59,150
4845 Pearl East Circle, Suite 300
Boulder, Colorado 80301
Tele: (720) 931-3038
Fax: (720) 931-3001